(815 ILCS 530/) Personal Information Protection Act

The Personal Information Protection Act became effective January 1, 2006.

The law requires "data collectors" that own or licenses personal information for any Illinois resident to notify the Illinois resident if there has been any "breach" in the "data collectors" computer systems.

A "data collector" may include but is not limited to, government agencies, public and private universities, privately and publicly held corporations, financial institutions, retail operators, and any other entity that, for any purpose, handles, collects, disseminates, or otherwise deals with nonpublic "personal information".

"Breach of the security of the system data" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of "personal information" maintained by the data collector.

"Personal information" means an individual's first name or first initial and last name in combination with any one or more of the following elements, when either the name or the data elements are not encrypted or redacted:

1. **Social Security number.**
2. **Driver's license number or State identification card number**
3. **Account number or credit or debit card number, or an account number or credit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account.**

"Personal information" does not include publicly available information that is lawfully made available to the general public from federal, State, or local government records.

Any data collector that owns or licenses personal information concerning an Illinois resident must notify that resident at no charge that there has been a breach of the security of the system data following discovery. The disclosure notification shall be made in the most expedient manner and without unreasonable delay.

Additionally, any "data collector" that maintains, but does not own or license "personal information" is required to notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if it was, or is reasonably believed to have been acquired by an unauthorized person.

The notification required may be delayed if an appropriate law enforcement agency determines that notification will interfere with a criminal investigation and provides the data collector with a written request for the delay. However, the data collector must notify the Illinois resident as soon as notification will no longer interfere with the investigation.

The Act also outlines the methods in which notice to Illinois residents is to be made. Permitted methods of notice include written notice; electronic notice if it complies with the federal digital signature statue; or substitute notice if the data collector demonstrates that the cost of providing notice would exceed $250,000 or there are more than 500,000 Illinois residents affected.

Substitute notice shall consist of all of the following:

(1) Email notice if the data collector has an email address for the subject persons.
(2) Conspicuous posting of the notice on the data collector's web site.
(3) Notification to major statewide media.

The Personal Information Act also allows a data collector to establish its own notification procedures, provided that the procedures are consistent with the notice timing under the Act.

A violation of the Act is deemed to be a violation of the Illinois Consumer Fraud and Deceptive Practices Act and could result in civil money penalties.

For information on what to do if your bank has suffered a security breach and what tell your customers: Go to http://www.fdic.gov/news/news/financial/2005/fil2705.html or http://www.fdic.gov/news/news/financial/2007/fil07032.html

For information on what to do if you believe you may be a victim of identity theft: Go to: http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt04.htm